* **PC机与RFID的通信**

PC机与RFID模块之间的通信采用UART，实现PC机对RFID模块的控制，从而实现标签的读数据、写数据操作。

PC机和RFID模块的通信采用面向字节的异步通信协议数据格式。规定主机发给RFID模块的数据帧为命令，RFID模块返回给主机的数据帧为响应。命令或响应数据帧是变长字节数，采用组包方法并用异或校验方法进行检错。

通信协议采用如图所示的层次结构，包括物理层、数据链路层和应用层。

|  |
| --- |
| 应用层 |
| 数据链路层 |
| 物理层 |

本协议对物理层和数据链路层进行了定义。

物理层完成信号的比特数据发送与接收，RFID模块和PC机之间的通信采用RS-232作为其物理层。其中，RS-232接口具体设计要求如下：

1、1位起始位、8位数据位、1位停止位、无奇偶校验位。

2、通信波特率设计为9600bit/s。

数据链路层具体规定命令帧和响应帧的类型与数据格式。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| D\_LEN  1Byte | 设备类型  1Byte | 消息ID  2Bytes | 流水号  4bytes | DATA | CHECK  1byte |

1、D\_LEN：该字段长度为1字节，表示DATA部分的长度。

2、设备类型：区分ZigBee、RFID等不同设备；RFID：0x01；ZigBee：0x02。

3、消息ID，区分不同设备的消息类型，不同设备类型的ID可以重复；

RFID 消息ID定义如下：

上位机请求帧：

0x00A0读卡号

0x00A1读数据

0x00A2写数据

0x00A3消费

0x00A4充值

0x1234设备状态

下位机响应帧：

0xA000读卡号

0xA100读数据

0xA200写数据

0xA300消费

0xA400充值

4、流水号：收到一条请求消息，要以同样的流水号回响应消息。

5、DATA为数据部分。RFID部分数据格式定义如下：

|  |  |  |
| --- | --- | --- |
| 上位机请求帧 | | |
| 消息ID  （2字节） | 对应操作  类型 | 消息体（DATA） |
| 00 A0 | 读卡号 | A0 + 数据长度（1字节） |
| 00 A1 | 读数据 | A1 + 密码（6字节）+ 块号（1字节） + 数据长度（1字节） |
| 00 A2 | 写数据 | A2 + 密码（6字节）+ 块号（1字节） + 数据长度（1字节）+ 数据（16字节） |
| 00 A3 | 消费 | A3 + 密码（6字节）+ 块号（1字节） + 数据长度（1字节）+ 数据（4字节） |
| 00 A4 | 充值 | A4 + 密码（6字节）+ 块号（1字节） + 数据长度（1字节）+ 数据（4字节） |
| 12 34 | 设备状态 |  |
|  |  |  |
| 下位机响应帧 | | |
| 消息ID  （2字节） | 对应操作  类型 | 消息体（DATA） |
| A0 00 | 读卡号 | A0 + 数据长度（1字节）+ 卡片序列号（4字节） |
| A1 00 | 读数据 | A1 + 块号（1字节） + 数据长度（1字节）+ 数据（16字节） |
| A2 00 | 写数据 | A2 + 块号+ 数据长度（1字节） |
| A3 00 | 消费 | A3 + 块号 + 数据长度（1字节）+ 数据（4字节） |
| A4 00 | 充值 | A4 + 块号 + 数据长度（1字节）+ 数据（4字节） |

* **调试**

在调试单机版RFID时，可以使用串口调试助手向RFID发送数据。串口调试助手和RFID之间的串口通信速率是9600，配置如下。应勾选“十六进制显示”和“十六进制发送”。



1、读取卡号

串口调试助手发送数据为：

02 02 00 A0 05 00 00 00 A0 00 01

返回：

06 00 A0 00 00 00 00 00 A0 04 39 69 40 A8 BA

2、读数据

串口调试助手发送数据为：

09 02 00 A1 05 00 00 00 A1 FF FF FF FF FF FF 0C 00 01

返回：

13 00 A1 00 00 00 00 00 A1 0C 10 00 00 00 00 FF FF FF FF 00 00 00 00 0C F3 0C F3 0F

3、写数据

串口调试助手发送数据为：

18 02 00 A2 05 00 00 00 A2 FF FF FF FF FF FF 0C 10 00 00 00 00 FF FF FF FF 00 00 00 00 0C F3 0C F3 01

返回：

03 00 A2 00 00 00 00 00 A2 0C 00 0F

4、消费

串口调试助手发送数据为：

0D 02 00 A3 05 00 00 00 A3 FF FF FF FF FF FF 0C 04 64 00 00 00 01

返回：

07 00 A3 00 00 00 00 00 A3 0C 04 00 00 00 00 0F

5、充值

串口调试助手发送数据为：

0D 02 00 A4 05 00 00 00 A4 FF FF FF FF FF FF 0C 04 64 00 00 00 01

返回：

07 00 A4 00 00 00 00 00 A4 0C 04 64 00 00 00 6B